

KNOW YOUR CUSTOMER (KYC) POLICY

RAPTURE B.V.

a Company with registered address at
Kaya Richard J. Beaujon Z/N Landhuis Joonchi II Curacao,
registration number 156074, domain name zaza.com
(hereinafter referred to as “**Company**”)

Stanislav Andrieiev, the
MLRO & Compliance
Officer

**Gouloud Mercedes
Hammoud** obo Guardian
Corporation Curacao B.V.,
Statutory Director

CONTENTS

1. GENERAL PROVISIONS AND POLICY STATEMENT.....	4
2. AUDIENCE.....	4
3. DEFINITIONS AND ABBREVIATIONS.....	5
4. CUSTOMER RISK ASSESSMENT	7
5. CUSTOMER ACCEPTANCE POLICY	7
6. CUSTOMER KYC	8
7. AWARE POLICY	11
8. RELIANCE ON THIRD PARTIES TO PERFORM KYC	11
9. REPORTING OF SUSPICIONS	11
10.RECORDING AND REPOTING.....	12
11.COOPERATION WITH AUTHORITIES	14
12.NOTIFICATIONS	14
13.UPDATING POLICIES AND PROCEDURES. RELATED INFORMATION.....	14
14.CONTACT INFORMATION.....	15
15.POLICY HISTORY.....	15

KEY INFORMATION

Approving Official(s):	Stanislav Andrieiev, the MLRO & Compliance Officer Gouloud Mercedes Hammoud obo Guardian Corporation Curacao B.V., the Statutory Director
Responsible Office:	Stanislav Andrieiev, the MLRO & compliance officer
Effective Date:	17.06.2025
Next Review Date:	17.06.2026

1. GENERAL PROVISIONS AND POLICY STATEMENT

- 1.1. The Company is dedicated to conducting its operations with the highest ethical standards and in strict compliance with all applicable laws and regulations related to financial transactions. In line with this commitment, all Customers are required to provide complete and accurate identification information during the registration process.
- 1.2. The Company reserves the right to verify Customer identities through reliable and independent sources. We are responsible for maintaining the accuracy and currency of all identification data. Should any inconsistencies or changes arise, the Company may update the relevant information accordingly.
- 1.3. Our Know Your Customer (KYC) Policy is a cornerstone of our efforts to uphold the integrity and security of our online gambling operations. It outlines the procedures and controls in place to verify Customer identities, ensure regulatory compliance, and prevent fraudulent activities, including money laundering and the financing of terrorism.
- 1.4. The primary goal of this Policy is to shield the Company from potential legal and regulatory risks by thoroughly assessing each Customer. This verification process confirms the identity and legitimacy of every user, discourages unlawful use of the platform, and fosters greater transparency and trust.
- 1.5. This Policy applies to all individuals who wish to register and participate in gaming activities on our Website. It includes procedures for Customer identification, verification, and the ongoing monitoring of account activity.
- 1.6. This Policy shall be in use with our General AML Policy, General AML Guide, Information Security Policy and any other internal regulation of our Company issued from time to time.
- 1.7. *Policy Scope and Applicability.* This KYC Policy, along with the associated procedures and internal controls, is designed to ensure compliance with all relevant regulations, including those set forth by the Financial Action Task Force (FATF), the Gaming Control Board (GCB), and general Anti-Money Laundering (AML) requirements. The Policy will be regularly reviewed and updated to reflect changes in applicable laws and regulations, as well as any developments within the Company's business operations. This ensures that our compliance framework remains current, effective, and aligned with evolving regulatory expectations.
- 1.8. The Company is responsible for developing and delivering training programs for all personnel involved in conducting transactions as referenced in the NOIS and NORUT. These programs establish clear rules of conduct for employee behavior and provide ongoing education to enhance awareness of the Company's policies against money laundering and terrorist financing. The training is designed to ensure that all relevant staff understand their responsibilities and are equipped to comply with applicable regulations and internal procedures
- 1.9. The Company is entitled to engage third parties to perform certain functions related to KYC procedures subject to confidentiality.
- 1.10. No member of staff shall at any time disclose a money laundering suspicion to the person suspected, whether or not a Customer, or to any outside party. If circumstances arise that may cause difficulties with Customer contact, the member of staff must seek and follow the instructions of the Responsible person.

2. AUDIENCE

- 2.1. This policy affects and regulates:
 - 2.1.1. Casino Management and Staff. Senior management and operations staff are directly involved in implementing and overseeing KYC policies and procedures. This includes understanding the requirements, ensuring compliance, and creating a culture of vigilance and ethical conduct within the Company.
 - 2.1.2. Compliance Officers. Individuals responsible for developing, implementing, and monitoring our compliance program. They ensure that our Company adheres to relevant laws and regulations and often serve as the primary liaison between the casino and regulatory authorities.
 - 2.1.3. Technology and IT Teams. These teams implement and manage technology solutions that support Customers

monitoring, customer due diligence, and reporting systems essential for AML and CTM compliance.

- 2.1.4. Customers. Although not directly involved in policy creation, Customers are a crucial audience as policies impact their interaction with the casino and our Company. These policies ensure customer transactions are safe and legitimate, thus building trust in the casino's operations and our Company.
- 2.1.5. Investors and Stakeholders. Investors and our stakeholders have a vested interest in the compliance with KYC policies. Compliance can impact the casino's financial performance and reputation, directly affecting their investment.
- 2.1.6. Financial Institutions. Banks and financial partners that facilitate transactions for our online casino and require assurance that our Company follow robust KYC policies. This is crucial for maintaining banking relationships and ensuring smooth financial operations.
- 2.1.7. Legal Team. Our Legal team Responsible for advising on regulatory requirements and potential legal implications of policy breaches. They ensure that the casino's policies align with the current legal landscape and international standards.
- 2.1.8. Third-party suppliers, that facilitate any services and products for our Company.
- 2.2. These Know Your Customer (KYC) standards and procedures means that all members of staff at all levels actively participate in preventing the services of the Company from being exploited by criminals and terrorists for money laundering purposes. This participation has its objectives as:
 - 2.2.1. Ensuring full compliance with all applicable Anti-Money Laundering (AML) laws and regulations in the relevant jurisdictions.
 - 2.2.2. All employees are required to take proactive steps to prevent, detect, and promptly report to the designated Responsible Person any actual or suspected misuse of the Company, its personnel, facilities, or operations for the purposes of money laundering, terrorist financing, or other unlawful activities.
 - 2.2.3. All relevant personnel must participate in AML training programs to ensure a thorough understanding of their responsibilities under the FATF standards, these internal guidelines, and any updates to applicable AML legislation.
 - 2.2.4. The Company is committed to protecting itself and its employees from legal, regulatory, and supervisory risks that may arise from breaches of AML obligations.
 - 2.2.5. The Company will take all necessary measures to safeguard its reputation from potential damage resulting from any association with money laundering or terrorist financing activities.
- 2.3. This Policy will be reviewed regularly to ensure it remains aligned with current legal and regulatory requirements. An independent audit of KYC compliance will be conducted annually, and the findings and recommendations will be carefully evaluated. The Company will ensure that sufficient authority, personnel, and resources are allocated to support and strengthen its AML compliance framework.

3. DEFINITIONS AND ABBREVIATIONS

- 3.1. **AML** – Anti-Money Laundering.
- 3.2. **CFT** – Combating the Financing of Terrorism.
- 3.3. **CPF** – Combating the Proliferation Financing
- 3.4. **Company** –Rapture B.V., a legally registered entity under the laws of Curaçao (registration no. 156074), located at Kaya Richard J. Beaujon Z/N Landhuis Joonchi II, Curaçao
- 3.5. **GCB** – Gaming Control Board of Curacao.
- 3.6. **POCA** – The Proceeds of Crime Act.
- 3.7. **OFAC** – Office of Foreign Assets Control.
- 3.8. **SDN** – Specially Designated Nationals and Blocked Persons list ("SDN List").

- 3.9. **FATF** – Financial Action Task Force. An independent intergovernmental body, established in 1989 and mandated by its Member Jurisdictions to develop and promote policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.
- 3.10. **XCG** – Caribbean Guilder, the currency of Curaçao.
- 3.11. **NOIS** – National Ordinance on Identification when rendering Services (Landsverordening identificatie bij dienstverlening, N.G. 2010, no. 40 as last amended by N.G. 2015, no. 69).
- 3.12. **NORUT** – National Ordinance on the Reporting of Unusual Transactions (Lands- verordening Melding Ongebruikelijke Transacties, N.G. 2010, no. 41 as last amended by N.G. 2015, no. 68).
- 3.13. **FIU** – The Financial Intelligence Unit Curacao.
- 3.14. **PEP** – is defined as an individual who is or has been entrusted with prominent public functions, excluding middle-ranking or more junior officials. This includes, but is not limited to, the following categories:
- Heads of State, Heads of Government, Ministers, and Deputy or Assistant Ministers;
 - Members of Parliament or equivalent legislative bodies;
 - Senior officials of political parties, including members of their governing bodies;
 - Members of supreme courts, constitutional courts, or other high-level judicial bodies whose decisions are generally not subject to further appeal, except under exceptional circumstances;
 - Members of courts of auditors or boards of central banks;
 - Ambassadors, chargés d'affaires, and senior-ranking officers in the armed forces;
 - Members of administrative, management, or supervisory boards of state-owned enterprises;
 - Directors, deputy directors, and members of the board or persons performing equivalent functions in international organizations.

In addition, the following individuals are also considered PEPs due to their relationship or association with the persons listed above:

- **Family members**, including spouses, partners, children and their spouses or partners, and parents;
 - **Close associates**, including individuals with joint beneficial ownership of legal entities or arrangements with a PEP, those with close business relationships with a PEP, or persons who are sole beneficial owners of entities or arrangements established for the benefit of a PEP.
- 3.15. **Gambling or Gambling Game** —Any online game made available on the Website that involves participation for the opportunity to win a Prize shall be considered a game of chance. A game of chance includes:
- (i) a game that contains elements of both chance and skill;
 - (ii) a game where the element of chance may be overcome or minimized through exceptional skill;
 - (iii) a game that is marketed or presented as involving an element of chance, excluding any activity classified as a sport.
- 3.16. **Reporting Form** – the standard form, issued by the FIU for the purpose of recording the information regarding an unusual transaction.
- 3.17. **Customer** — an individual, who uses the Website and/or familiarizes himself with the provisions of the Website, these Policy and the provisions of other documents, and intends to register on the Website to participate in Gambling (acquire a Player status).
- 3.18. **Third Parties** — any individuals and/or legal entities other than the User and/or the Player, in particular, but not exclusively: family members, spouses, friends, partners, counterparties, creditors, service providers, agents, etc.
- 3.19. **Website** — the official websites of the Company, on which Customer may play the Gambling Games.
- 3.20. In this Policy singular include the plural, and the plural include singular in cases of a need for interpretation.

POLICY IMPLEMENTATION

4. CUSTOMER RISK ASSESSMENT

- 4.1. Customer risk refers to the potential threat of money laundering (ML) or terrorist financing (TF) associated with establishing and maintaining a business relationship with an individual Customer or group of Customers. Assessing this risk is a fundamental element of the Company's risk-based approach to compliance.
- 4.2. The Company employs defined criteria to evaluate whether a Customer poses an elevated level of risk and considers relevant mitigating factors that may influence this assessment. Risk variables—such as a Customer's economic activity, source of funds or wealth, geographic location, and transaction behavior—may increase or decrease the overall level of assessed risk. Certain categories of Customers may inherently present a higher risk due to the nature of their activities. These include, but are not limited to:
 - 4.2.1. Customers who have multiple sources of income;
 - 4.2.2. Customers with irregular income streams;
 - 4.2.3. PEPs;
 - 4.2.4. High spenders (money can be derived from illegal activities);
 - 4.2.5. Disproportionate spenders (inconsistent with our Company's information about the source of wealth or income);
 - 4.2.6. Improper use of third parties, criminals use third parties to gamble and break up large amounts of cash, to buy chips or to cash out on behalf of others to avoid KYC measures;
 - 4.2.7. Customers using multiple casino player rating accounts to hinder a casino to track their gambling activities;
- 4.3. The Company establishes a benchmark value to define the upper limit of typical transaction amounts. This benchmark serves as a reference point for identifying unusual or potentially suspicious activity. Customers with a single, stable source of income are generally deemed to present a lower risk of money laundering or terrorist financing, while those with multiple, inconsistent, or unexplained income streams may be classified as higher risk.

5. CUSTOMER ACCEPTANCE POLICY

- 5.1. The Customer Acceptance Policy defines the criteria used to determine whether a Customer is eligible to establish an account with the Company. It also outlines the circumstances under which enhanced due diligence measures are required, particularly in cases where a Customer is assessed as having an elevated risk profile.
- 5.2. Prohibited Customers include:
 - 5.2.1. Individuals who refuse to provide necessary information or documentation, do not supply sufficient information, fail to disclose their identity, or where KYC processes cannot be carried out.
 - 5.2.2. Individuals who provide False Information.
 - 5.2.3. Individuals who use aliases, hide their real names, or give false information to mask their identity.
 - 5.2.4. Individuals who appear on sanction lists issued by the Money Laundering Officer (MLRO) or international organizations.
 - 5.2.5. Individuals suspected of using the Company for money laundering, terrorist financing, or financing the proliferation of weapons of mass destruction.
 - 5.2.6. Individuals under the legal age of 18 (or the age of majority in their jurisdiction). Anyone under eighteen cannot be registered as a Player, and any deposits or winnings from such individuals will be forfeited to the Regulatory Authority.
 - 5.2.7. Politically Exposed Persons (PEPs). These are individuals with prominent political roles or high-profile public functions, presenting a greater risk of involvement in money laundering or terrorist financing due to their positions.

6. CUSTOMER KYC

- 6.1. The Company is entitled to conduct the Customer "Know Your Customer" measures when:
 - 6.1.1. Establishing business relations.
 - 6.1.2. Withdrawing from business relations.
 - 6.1.3. Carrying out occasional transactions on and/or above the monetary equivalent of EUR 2 200, or the equivalent of XCG 4 000 in currency available on the Website (Enhanced due diligence shall be performed in this case).
 - 6.1.4. There is a suspicion of money laundering or terrorist financing.
 - 6.1.5. The Company has doubts about the veracity or adequacy of previously obtained Customer identification data.
- 6.2. The Company conducts the KYC:
 - 6.2.1. To identify the Customer and verify that Customer's identity using reliable, independent source documents, data or information.
 - 6.2.2. To identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner.
 - 6.2.3. To understand and, as appropriate, to obtain information on the purpose and intended nature of the business relationship.
 - 6.2.4. When identifying the Customer, at a minimum the following information must be collected: full name; permanent residential address; date of birth; place of birth; nationality; identity number.
- 6.3. To carry out the KYC the Company is entitled to receive from the Customer-individual the following documents: (i) an ID card, or (ii) a passport, or (iii) a driver's license.
- 6.4. In addition, the Company is entitled to receive from the Customer the following documents (in case of Enhanced Due Diligence): (i) a birth certificate, (ii) residence permit, (iii) tax bills, (iv) utility bills, (v) bank, building society or credit union statement or passbook containing current address.
- 6.5. The Company's Customer Identification Procedures are based on the principle that funds will only be accepted from new or existing Customers after their identity has been verified and it is confirmed that they are acting on their own behalf. In cases where a Customer is acting on behalf of a third party, this relationship must be fully disclosed, and the Company must verify the identity of the underlying third party before proceeding with the transaction or account activity.
- 6.6. Customer Identification Procedures must be tailored to reflect the specific characteristics and risk profile of each Customer. The designated Responsible Person may determine that enhanced KYC measures are warranted in certain cases, based on the circumstances and associated risk factors.
- 6.7. An Individual Customer KYC Checklist is used as a practical reference to guide the identification process. Staff are encouraged to submit any suggestions for updates or improvements to the Responsible Person for review and possible inclusion.
- 6.8. The Responsible person shall retain copies of all documents reviewed or checklists completed in connection with its Customer Identification Procedures in accordance with Company's Customer Records Retention policies.
- 6.9. If a Customer is unable to provide acceptable identification documents, the responsible staff will make a risk-based decision regarding the acceptance of the available documentation, consulting with the Responsible Person as needed.
- 6.10. When the Customer is not the beneficial owner of the assets involved, the responsible staff must take appropriate steps to identify the beneficial owner and apply reasonable measures to verify their identity.
- 6.11. The Responsible Person will develop a standardized format for use by responsible staff when requesting identity and beneficial ownership verification from relevant corporate entities and trustees, as well as procedures for

follow-up if responses are not received within the required statutory timeframe.

- 6.12. If all reasonable efforts to identify the beneficial owner of a Customer entity have been exhausted and properly documented without success, the responsible staff must seek approval from the designated Responsible Person. Such approval may be granted based on a risk-sensitive assessment, allowing the designation of the individual who exercises ultimate effective control over the Customer entity as the beneficial owner.
- 6.13. In any case where a heightened risk of money laundering is identified and enhanced due diligence is required, the Responsible Person shall consult with Management to determine any additional verification measures necessary to confirm the Customer's identity.
- 6.14. All actions taken during the identity verification process, including those related to corporate entities, must be thoroughly documented. This includes retaining photocopies of identification documents or, in exceptional cases and with Management's approval, recording details of where such documents are stored and can be accessed.
- 6.15. The Company reserves the right to verify whether an individual is acting on their own behalf or on behalf of another party. If acting on behalf of a third party, the Company is entitled to establish the identity of that third party using the documentation provided. If that third party is, in turn, acting for another party, the Company may also establish the identity of the next-level third party, continuing as necessary.
- 6.16. If the Company knows or has reasonable grounds to suspect that an individual is not acting on their own behalf, it is authorized to take appropriate steps to identify the actual Customer and, where relevant, the third-party representative acting on the Customer's behalf.
- 6.17. Verification of an identity refers to actions taken to verify that a person exists and is who he claims to be. This is done by checking reliable, independent (of the person whose identity is being verified) sources.
- 6.18. The Company is entitled to record the following data in such a manner that they are accessible:
 - 6.18.1. The name, the address, the identification information from an (i) ID card, or (ii) a passport, or (iii) a driver's license, the residence or place of establishment of the Customer and the ultimate interested party, if there is any, and/or the person in whose name a payment or transaction is made, and also of their representatives.
 - 6.18.2. The nature, the number and the date and place of issue of the document with the help of which the identification has taken place.
 - 6.18.3. Current and past addresses, date of birth, place of birth, physical appearance, employment and financial history, family circumstances.
 - 6.18.4. Phone number, Email address, mailing address, other contacts.
- 6.19. The Company may employ trustworthy electronic systems to support the verification of Customer identities. These systems often provide the added capability of identifying Politically Exposed Persons (PEPs). Electronic data sources can offer comprehensive verification without requiring Customers to submit physical documentation. Depending on the assessed risk level, electronic verification may be used independently or in combination with traditional document-based methods. For electronic checks to be accepted as standalone proof of identity, they must: (i) aggregate data from multiple independent sources over a period of time, and (ii) include qualitative assessments to determine the reliability and credibility of the information obtained.
- 6.20. The Company has the right to obtain or review original documents and verify their authenticity by referencing authoritative sources that detail security features designed to prevent forgery. Additionally, the Company may compare the individual presenting or providing the document with the document itself—for example, by matching the photograph or verifying other identifying information.
- 6.21. If the Company has any doubts regarding the authenticity of documents submitted by a Customer, it reserves the right to conduct electronic verification using a system capable of reliably confirming the Customer's identity—not just their existence. In addition, the Company may seek relevant information from other regulated institutions, such as banks, to supplement existing documentation and data. This approach supports the ongoing validation of the Customer's legitimacy and may yield either confirming or disqualifying results.

- 6.22. Before opening an account, and on an ongoing basis, the Company will check to ensure that a Customer does not appear on the SDN list or is not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC. (See the OFAC website for the SDN list and listings of current sanctions and embargoes). Because the SDN list and listings of economic sanctions and embargoes are updated frequently, we will consult them on a regular basis and subscribe to receive any available updates when they occur. With respect to the SDN list, we may also access that list through various software programs to ensure speed and accuracy. See also OFAC's Sanctions List Search tool, which screens names against the SDN list and other sanctions lists administered by OFAC. The Company will also review existing accounts against the SDN list and listings of current sanctions and embargoes when they are updated and [he or she] will document the review.
- 6.23. The Company does not permit accounts to be opened by, or to make any deposits nor used from, customers located or domiciled in Afghanistan, Algeria, Angola, American Samoa, Aruba, Australia, Antigua and Barbuda, Bahamas, Barbados, Belize, Bermuda, Belgium, Bonaire, Bosnia and Herzegovina, Bolivia, Burma/Myanmar, Burundi, Burkina Faso, Bulgaria, Cameroon, Central African Republic, Curaçao, Côte d'Ivoire, China, Denmark, Democratic Republic of the Congo, Egypt, Eritrea, Estonia, France, French Guyana, Greenland, Guadeloupe, Guam, Guatemala, Haiti, Holy See (Vatican City), Jamaica, Italy, Iran, Iraq, ISIL and Al-Qaida, Ivory Coast, Kenya, Lao People's Democratic Republic, Lebanon, Libya, Lithuania, Kuwait, Malaysia, Marshall Islands, Martinique, Maldives, Mali, Monaco, Mozambique, Namibia, Nepal, Netherlands, North Korea (Democratic People's Republic of Korea), Occupied Palestinian Territory, Poland, Puerto Rico, Qatar, Reunion, Republic of Guinea, Saba, Saint Barthélemy, Saint Martin, Saint Pierre and Miquelon, Singapore, Spain, South Africa, Somalia, South Sudan, St. Eustatius, Sudan, Syria, Tunisia, Trinidad & Tobago, USA, US Minor Outlying Islands, Virgin Islands (UK), Venezuela, Vietnam, Yemen, Zimbabwe or countries that are placed by FATF to the "black list" of countries. It is prohibited to use our services and play Gambling Games from Curacao, therefore, access to our Website is prohibited from Curacao.
- 6.24. Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our Customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. The Company will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the Customer (e.g., whether the information is logical or contains inconsistencies).
- 6.25. The Company may rely on official documents to verify a Customer's identity when such documentation is available and appropriate. However, in light of the increasing prevalence of identity fraud, documentary verification will be strengthened with non-documentary methods whenever necessary. These alternative methods may also be applied if there is any residual uncertainty regarding the Customer's true identity. In conducting identity verification, the Company will evaluate whether the identifying information provided—such as full name, street address, postal code, telephone number (if available), date of birth, and Social Security number—forms a consistent and credible basis for a reasonable belief that the Customer's identity has been accurately established.
- 6.26. We acknowledge that we are not obligated to verify the validity of documents provided by Customers for identity verification and may rely on government-issued identification as sufficient proof of identity. However, if a document displays clear signs of fraud, we must take this into account when assessing whether we can reasonably believe that we have accurately identified the Customer.
- 6.27. The Company will verify Customer information within a reasonable timeframe prior to account activation. Depending on the nature of the account and the type or value of requested transactions, the Company may, at its discretion, decline to process a transaction until verification is complete. In certain cases, if additional time is required, the Company may impose temporary restrictions on transaction types or monetary limits pending verification. If, during the verification process, any information raises suspicion of potential money laundering, terrorist financing, or other illicit activity, the matter will be escalated internally to the AML Compliance Officer. Following this review, and in accordance with applicable laws and regulations, a Unusual Transaction Report (UTR) will be filed as appropriate.
- 6.28. The Company is entitled to engage third parties to conduct Customer Due Diligence subject to confidentiality.
- 6.29. The Customer checks shall be performed till the moment of receiving all needed documents and information according to this Policy or till the moment when the Customer rejects or unable to provide all needed documents and information for more than 2 weeks from the request date. When the Customer rejects or unable to provide all

needed documents and information for more than 2 weeks from the request date the AML specialist shall record the unusual and shall execute the measures that are provided in this Policy.

7. AWARE POLICY

- 7.1. All staff members must remain alert to any signs that the Company's services may be misused for money laundering purposes or that they may encounter criminal or terrorist property in the course of their duties.
- 7.2. If a staff member becomes aware of a potential suspicion, they must collect any relevant information that is routinely accessible and assess whether there are reasonable grounds to suspect money laundering. Any additional information obtained—particularly explanations for unusual instructions or transactions—should be documented in the Customer's file in the normal course of business. However, under no circumstances should any reference to suspected money laundering be included in the Customer file.
- 7.3. Staff are not required to conduct investigations or perform independent research. Their responsibility is limited to reviewing information sources that are readily available within the Company.
- 7.4. If, after reviewing the available information, the staff member is fully satisfied that no reasonable grounds for suspicion exist, no further action is necessary. However, if reasonable grounds are identified, the matter must be promptly escalated to the designated Responsible Person.
- 7.5. When a staff member, based on their own observations, determines that there are reasonable grounds to suspect money laundering, they must submit a formal internal suspicion report to the Responsible Person. This report must be prepared in the format prescribed by the Responsible Person. The submission of such a report does not constitute a breach of Customer confidentiality.
- 7.6. A member of staff who forms or is aware of a suspicion of money laundering shall not discuss it with any outside party, or any other member of staff unless directly involved in the matter causing suspicion.
- 7.7. No member of staff shall at any time disclose a money laundering suspicion to the person suspected, whether or not a Customer, or to any outside party. If circumstances arise that may cause difficulties with Customer contact, the member of staff must seek and follow the instructions of the Responsible person.

8. RELIANCE ON THIRD PARTIES TO PERFORM KYC

- 8.1. The Company may, under certain conditions, rely on third parties to carry out specific Know Your Customer (KYC) procedures, provided that the requirements outlined in this Policy are fully met. Any third party engaged for this purpose must be subject to KYC and record-keeping obligations equivalent to those applicable to the Company, and must have an established, independent business relationship with the Customer outside the relationship the Customer seeks to form with the Company. While such reliance is permitted, the Company retains ultimate responsibility for ensuring that all KYC requirements are fulfilled. To that end, a formal agreement must be in place with the third party, ensuring that copies of identification data and other relevant documentation can be provided upon request. This arrangement must be periodically reviewed and tested to confirm its effectiveness.

9. REPORTING OF SUSPICIONS

- 9.1. If the Company suspects or has reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts, or terrorist organizations, it shall promptly report its suspicion to the FIU in accordance with art. 11 of the NORUT.
- 9.2. By virtue of article 11 of the NORUT, the Company shall report any unusual transaction or any intended unusual transaction to the FIU without delay. Unusual transactions shall be reported in compliance with the NORUT.
- 9.3. The following transactions or intended transactions are deemed unusual:
 - 9.3.1. Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance
 - 9.3.2. Transactions which in connection with money laundering or terrorism financing are reported to the police authorities or to the following department of justice.

- 9.3.3. We may file a voluntary FIU for any unusual transaction that we believe is relevant to the possible violation of any law or regulation but that is not required to be reported by us under the FIU rule. It is our policy that all FIU will be reported regularly to the Board of Directors and appropriate senior management, with a clear reminder of the need to maintain the confidentiality of the FIU.
- 9.3.4. We will retain copies of any FIU filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the forms. We will identify and maintain supporting documentation and make such information available to any appropriate law enforcement agencies, state regulators upon request.

10. RECORDING AND REPOTING

- 10.1. Each unusual transaction is documented individually by the Company using a designated Reporting Form, which is assigned a unique, consecutive number for tracking purposes. In the event a Reporting Form is voided, it will still be retained and properly archived by the Company to ensure comprehensive record-keeping.
- 10.2. The Company maintains comprehensive records containing all information and documentation necessary to demonstrate compliance with the KYC measures outlined in this Policy. These records also capture the background and intended purpose of relevant transactions. All such documentation is retained for a minimum period of five years from the date the business relationship ends or from the date of any occasional transaction, whichever is applicable.
- 10.3. Each report about an unusual transaction will include at least the following information:
 - 10.3.1. The identity of the Customer.
 - 10.3.2. Nature and number of the identification document of the Customer.
 - 10.3.3. The nature, date, time and place of transaction.
 - 10.3.4. The amount, destination and origin of the funds, securities, precious metals, or other values involved in the transaction
 - 10.3.5. The circumstances that identified the transaction as unusual.
- 10.4. The Compliance Officer signs the reporting form if it is submitted manually.
- 10.5. The senior management (director, executive director, CEO, etc.) is entitled to sign the reporting form with the verbal consent of the Compliance Officer.
- 10.6. In accordance with Article 11 of the NORUT, the Company is required to report any unusual transaction or any attempted unusual transaction to the Financial Intelligence Unit (FIU) without delay. To facilitate this, the Company must establish clear procedures for both internal and external reporting of unusual transactions, and ensure these procedures are effectively communicated to all relevant personnel. All unusual transactions—whether single occurrences or a series of related transactions as outlined in the Policy’s Unusual Transaction Indicators—must be reported internally immediately. Additionally, all relevant supporting documentation must be submitted alongside the report to enable thorough review and timely action.
- 10.7. The Company may submit reports using an electronic system approved by the Financial Intelligence Unit (FIU) or, alternatively, provide a paper copy of the reporting form. For data security reasons, submission of paper forms via fax is prohibited. Regardless of the submission method, the Company will retain a copy of each reporting form in its records. These records must be made available to agents of the Gaming Control Board (GCB) upon request.
- 10.8. The Company shall provide information and documentation related to its money laundering and terrorist financing policies, as well as deterrence and detection procedures, to the examiners of the GCB both during

examinations and upon request throughout the year.

- 10.9. The Company making the following documents and information readily available:
 - 10.9.1. Its written and approved policy and procedures on money laundering and terrorist financing prevention.
 - 10.9.2. The name of each Compliance Officer responsible for the Company's overall money laundering and terrorist financing deterrence and detection procedures and her/his designated job description.
 - 10.9.3. Records of reported unusual transactions
 - 10.9.4. Records on unusual transactions which required closer investigations.
 - 10.9.5. The completed source of funds declaration.
 - 10.9.6. Schedule of the training provided to our personnel regarding money laundering and terrorist financing.
 - 10.9.7. The assessment report on the Company's policies and procedures on money laundering and terrorist financing by the internal audit department or the Company's external auditor.
 - 10.9.8. Required copies of identification documents.
- 10.10. The listing above is not limitative and does not exclude the Company from providing additional information and documentation if the GCB so requests.
- 10.11. In addition, the Company maintain a record in writing of its (i) policies, procedures and controls, (ii) any changes to those policies, procedures and controls, (iii) the steps the Company have taken to communicate the policies, procedures and controls or any changes to them, within the Company's business.
- 10.12. The Company may share information about individuals, entities, organizations, and countries with financial institutions or government authorities to assist in identifying and, where appropriate, reporting suspected terrorist activities or money laundering. Prior to sharing such information, the Company will take reasonable steps to verify that the recipients are authorized to receive it under applicable laws and regulations.
- 10.13. We will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information.
- 10.14. We also will employ procedures to ensure that any information received from another financial institution shall not be used for any purpose other than:
 - 10.14.1. Identifying and, where appropriate, reporting on money laundering or terrorist activities;
 - 10.14.2. Determining whether to establish or maintain an account, or to engage in a transaction; or
 - 10.14.3. Assisting the financial institution or gambling operator in complying with performing such activities.
- 10.15. If we determine that a customer is on the SDN list or is engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC, we will reject the transaction and/or block the customer's assets and file a blocked asset and/or rejected transaction form with OFAC within 10 days.
- 10.16. Our Company is obligated not only to comply with the National Ordinance for Identification of Services but also to detect and report both intended and completed unusual transactions. We have established adequate procedures covering: (i) the identification of unusual transactions, (ii) the documentation of such transactions, and (iii) the reporting process for unusual transactions.
- 10.17. An unusual transaction is characterized by a departure from the Customer's established profile. Effectively identifying such transactions requires the Company to have comprehensive knowledge of the Customer. By collecting relevant Customer information, the Company can document and evaluate the associated risks and develop a behavioral profile that anticipates expected transaction patterns within the business relationship. In line with NORUT legislation, the Company utilizes both objective and subjective indicators to assist in determining whether a Customer's transaction should be classified as unusual.
- 10.18. Management ensures that all staff receive specific guidance and training to identify and accurately document unusual transactions. Every such transaction must be reported to the Compliance Officer using the management-

approved reporting format. Supporting documents—such as copies of identification, cash-out slips, and other pertinent records—must accompany the report. The Compliance Officer is responsible for maintaining a well-organized filing system for all related records. In cases where internally reported transactions are not escalated to the Financial Intelligence Unit (FIU), the reasons for withholding must be fully documented and approved by the Compliance Officer and/or management.

- 10.19. In order to implement FAT recommendation, Our Company pays special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The following transactions or intended transactions are deemed unusual:
 - 10.19.1. Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
 - 10.19.2. Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
 - 10.19.3. Transactions in the amount of equivalent of XCG 5,000 or more, regardless of whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means. This includes but is not limited to: A cashless transaction in the amount of equivalent of XCG 5,000 or more. A cashless transaction is a transfer from a bank account of the Company to a local or international bank account, at the request of the Customer. Accepting or releasing a deposit in the amount of equivalent of XCG 5,000 or more at the request of the Customer.
- 10.20. A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount of the monetary equivalent of XCG 5,000 or more and is considered per gaming day.
- 10.21. Our Company registered with the FIU and to obtain access to the goAML reporting portal after validation by the FIU. The FIU allows bulk reporting, therefore our account manager at the FIU should be contacted in order for the FIU to determine if the operator qualifies for this service.

11. COOPERATION WITH AUTHORITIES

- 11.1. The Company commits to fully cooperate with law enforcement and regulatory authorities by providing requested information within five (5) business days, unless otherwise specified by the requesting authority.
- 11.2. The Compliance Officer shall act as the primary liaison for all communications and requests from such authorities.

12. NOTIFICATIONS

- 12.1. The Company is entitled to provide notice to Customers that the Company is requesting information from them to verify their identities, as required by the legislation.
- 12.2. The Company is entitled to provide any other notices to Customer, for example – termination notice, notice of blocking of the account, warning notice, etc.
- 12.3. We will use the following method to provide notices to customers – Email notice and/or phone call and/or internal account notice and/or mail notice.

13. UPDATING POLICIES AND PROCEDURES. RELATED INFORMATION

- 13.1. The Company is required to check for amendments on Sanctions Decrees and Regulations on a regular basis and update the KYC policies and – procedures accordingly to reflect such amendments. Such information contains lists of suspected terrorists, terrorist groups, and associated individuals and entities as mentioned in (in any case):
 - 13.1.1. The Consolidated United Nations Security Council Sanctions List.

- 13.1.2. The Sanction Decree “Al-Qaida c.s., the Taliban of Afghanistan c.s., ISIL c.s., ANF c.s.” (N.G. 2015, no. 29).
- 13.1.3. The Ministerial Regulation “Libya” (N.G. 2015, 28).
- 13.1.4. The Sanction Decree “Islamic Republic Iran 2015” (N.G. 2015, 27).
- 13.1.5. The Sanction Decree “Democratic People’s Republic of Korea 2015” (N.G. 2015, 30).
- 13.1.6. The Ministerial Regulation “Yemen” (N.G. 2015, 65).
- 13.1.7. Guidance for Financial Institutions in Detecting Terrorist Financing.
- 13.1.8. The listing¹³ of the Office of Foreign Assets Control (OFAC).
- 13.1.9. The National Ordinance on Identification of Customers when Rendering Services (N.G. 2017, no. 92).
- 13.1.10. The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99).
- 13.1.11. Ministerial Decree with general operation of November 11, 2015, laying down the indicators as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions.
- 13.1.12. (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73).
- 13.1.13. The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).
- 13.1.14. National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34).
- 13.1.15. National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council.
- 13.1.16. National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nation Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28).
- 13.1.17. Kingdom Sanction Act (N.G. 2016, no. 54).
- 13.1.18. National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2).
- 13.1.19. The National Ordinance on Identification of Customers when Rendering Services (N.G. 2017, no. 92).

14. CONTACT INFORMATION

14.1. For questions or further information regarding this policy, please contact:

 Email: support@zaza.group

 Address: Kaya Richard J. Beaujon Z/N Landhuis Joonchi II, Willemstad, P.O. Box 6248, Curacao

15. POLICY HISTORY

June 17, 2025	Policy update (Annual update)
December 01, 2024	Policy update (legal changes)
June 12, 2024	Policy update (legal changes)
May 28, 2024	Policy update (Annual update)
December 12, 2023	Policy update (legal changes)

May 20, 2023	Policy update (Annual update)
May 24, 2022	Initial Policy